

# SPYWOLF

**Security Audit Report** 



Completed on

December 4, 2023



# OVERVIEW

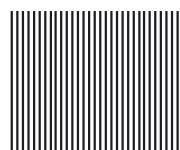
This audit has been prepared for **Santa Trump** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -







### TABLE OF CONTENTS

Drainat Description		01
Project Description		01
Contract Information		02
Current Stats		03
Vulnerability Check		04
Threat Levels		05
Found Threats	06-A/06-C	
Good Practices		07
Tokenomics		08
Team Information		09
Website Analysis		10
Social Media & Online Presence		11
About SPYWOLF		12
Disclaimer		13



# Santa Trump



### **PROJECT DESCRIPTION**

### According to their website:

Santa Trump is the first token on the Binance Smart Chain to directly support Donald Trump's 2024 presidential election.

Through our trading taxes, we will make verified donations to MAGA 2024 and help the greatest President of all time get back in office.

But in the spirit of Christmas, we won't forget our holders. Trump has donned his Santa suit and we will be rewarding YOU with YUUUUGE USDT rewards for holding the most hyped community token of 2023!

Release Date: Presale starts in December, 2023

Category: Meme token



### CONTRACT INFO

Token Name

Trump Santa

Symbol



**Contract Address** 

0x3248620b057303950f514421Ee9fd6DE816F8b97

Network

**Binance Smart Chain** 

Deployment Date

Dec 03, 2023

Total Supply

420,000,000,000,000

Language

Solidity

**Contract Type** 

Token with dividends

Status

Not launched

### **TAXES**

Buy Tax **5%** 

Sell Tax **5%** 



# Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

### Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

<sup>\*</sup>Taxes cannot be changed





### **TOKEN TRANSFERS STATS**

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	42000000000000000000000000000000000000
Median Transfer Amount	4200000000000 
Average Transfer Amount	4200000000000 
First transfer date	2023-12-03
Last transfer date	2023-12-03
Days token transferred	NTDACT STATS

### SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-12-03 09:33:43 UTC
Created	2023-12-03 09:33:43 UTC
Create TX	0x1a64d5c80b268ca56dca330e2dfdd70a51 b1cbfa260639cf92ef8ec7e5c39315
Creator	0xe91da8bfaf378aa8442536a307709e6fbf27 61ae





### **VULNERABILITY CHECK**

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

SPYWOLF.CO



### THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

### High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

### Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

### Low Risk

Issues on this level are minor details and warning that can remain unfixed.

### Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



### **FOUND THREATS**

### High Risk

tradingEnabled is currently false, allowing vetted addresses to potentially sell their presale tokens before opening trade for the investors.

Note: This only applies if launching on a launchpad platform like Pinksale.

```
function enableTrading() external onlyOwner{
   require(!tradingEnabled, "Trading already enabled.");
   tradingEnabled = true;
   swapEnabled = true;
function transfer(
   address from,
   address to,
   uint256 amount
   require(from != address(0), "ERC20: transfer from the zero address");
   require(to != address(0), "ERC20: transfer to the zero address");
   require(tradingEnabled || _isExcludedFromFees[from] || _isExcludedFromFees[to], "Trading not yet enabled!");
```

- Recommendation:
  - Once presale is finished and trading is not enabled, investors cannot sell their token holdings on token launch. Trading should be enabled before presale finish and token launch on DEX.





### Informational

Owner can exclude address from fees.

When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function excludeFromFees(address account, bool excluded) external onlyOwner {
    require(_isExcludedFromFees[account] != excluded, "Account is already set to that state");
    _isExcludedFromFees[account] = excluded;
    emit ExcludeFromFees(account, excluded);
}
```

Owner can withdraw any tokens from the contract except the native TrumpSanta token.

When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function claimStuckTokens(address token) external onlyOwner {
    require(token != address(this), "Owner cannot claim native tokens");
    if (token == address(0x0)) {
        sendBNB(payable(msg.sender), address(this).balance);
        return;
    }
    IERC20 ERC20token = IERC20(token);
    uint256 balance = ERC20token.balanceOf(address(this));
    ERC20token.transfer(msg.sender, balance);
}
```

06-B





### Informational

Owner can exclude address from dividends.

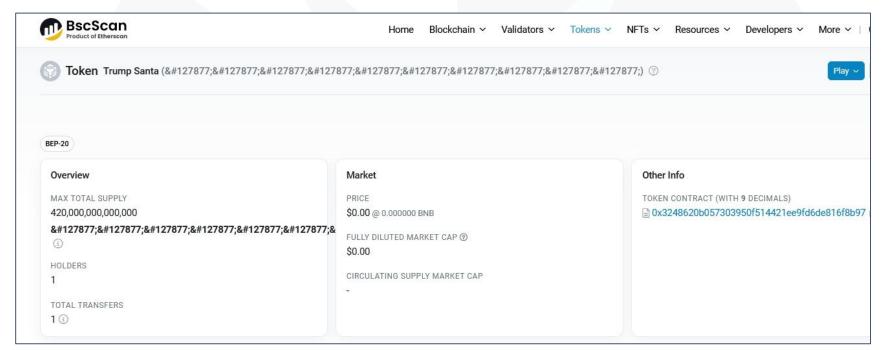
```
function excludeFromDividends(address account) external onlyOwner{
    dividendTracker.excludeFromDividends(account);
}

function excludeFromDividends(address account) external onlyOwner {
    require(!excludedFromDividends[account]);
    excludedFromDividends[account] = true;

    _setBalance(account, 0);
    tokenHoldersMap.remove(account);

emit ExcludeFromDividends(account);
}
```

Token's symbol may not be interpreted correctly by explorers and/or DEXes.







### RECOMMENDATIONS FOR

# GOOD PRACTICES

- Consider fundamental tradeoffs
- Be attentive to blockchain properties
- 3 Ensure careful rollouts
- 4 Keep contracts simple
- Stay up to date and track development

# Santa Trump GOOD PRACTICES FOUND

- The owner cannot mint new tokens after deployment
- The owner cannot stop or pause the contract
- The owner cannot set a transaction limit
- The smart contract utilizes "SafeMath" to prevent overflows

07



There is no information about the initial tokens distribution based on the project's whitepaper and/or website.

SPYWOLF.CO



# THE

1 The team is annonymous

### **KYC INFORMATION**

### No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



09





### **Website URL**

https://www.santatrump.us/

### Domain Registry https://www.godaddy.com

### **Domain Expiration**

2024-11-26

### **Technical SEO Test**

Passed

### **Security Test**

Passed. SSL certificate present

### Design

Single page design with appropriate color scheme and graphics.

### Content

The information helps new investors understand what the product does right away. No grammar mistakes found.

### Whitepaper

### Roadmap

No

### Mobile-friendly?



### santatrump.us

SPYWOLF.CO

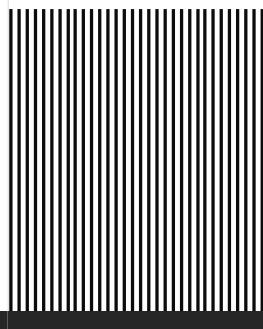
### F

## SOCIAL MEDIA

& ONLINE PRESENCE



Project's social media pages are new







### **Twitter**

@SantaTrump\_US

- No followers
- No posts
- New account



### Telegram

@SantaTrump\_US

- 7 members
- Active members



**Discord** 

Not available



Medium

Not available



# SPYWOLF CRYPTO SECURITY

Audits | KYCs | dApps Contract Development

### **ABOUT US**

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 700 SUCCESSFUL CLIENTS
- ✓ MORE THAN 1000 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to contact@spywolf.co or t.me/joe\_SpyWolf

### FIND US ONLINE



SPYWOLF.CO



@SPYWOLFNETWORK



@SPYWOLFNETWORK



### Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

### **DISCLAIMER:**

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.

